



Credit Union National Association

cuna.org

601 Pennsylvania Ave., NW | South Building, Suite 600 | Washington, DC 20004-2601 | **PHONE:** 202-638-5777 | **FAX:** 202-638-7734

VIA E-MAIL – Taskforcecomments@idtheft.gov

January 18, 2007

Identity Theft Task Force - P065410
Federal Trade Commission/Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580.

Re: Identity Theft Task Force

Dear Sir or Madam:

The Credit Union National Association (CUNA) appreciates the opportunity to respond to the request from the Federal Identity Theft Task Force (Task Force) for comment on methods for improving the effectiveness and efficiency of federal government efforts to reduce identity theft. CUNA represents approximately 90 percent of our nation's 8,700 state and federal credit unions, which serve nearly 87 million members.

Summary of CUNA's Comments

- CUNA fully supports the goals of the Task Force with regard to addressing identity theft issues, and CUNA has been proactive in these goals by providing education to our members and input to the government.
- The focus on efforts to address identity theft should include addressing security breach vulnerabilities, which should focus on efforts that merchants and processors need to undertake to address these problems.
- As it considers new requirements in this area, the federal government should take into account the significant regulatory requirements that have been imposed on financial institutions over the past several years, which include the Gramm-Leach Bliley Act, the Bank Secrecy Act, the USA PATRIOT Act, as well as the Fair and Accurate Credit Transactions Act (FACT Act). Any new requirements should be risk-based to take into account the size and complexity of those that must comply with these new requirements, and flexible in order to accommodate future changes in technology.



AMERICA'S
CREDIT UNIONS®

OFFICES: | WASHINGTON, D.C. | MADISON, WISCONSIN

- The federal government should undertake a periodic review of the burdens under the FACT Act, as well as other regulatory requirements in this area.
- CUNA strongly supports the efforts of law enforcement to prosecute those that commit identity theft and believe these efforts should be publicized in an effort to reassure the public.

Discussion

CUNA fully supports the goals of the Task Force, which is to develop a coordinated strategic plan to combat identity theft, and to recommend ways to improve the effectiveness and efficiency of the federal government's activities in many areas. These areas include identity theft awareness, prevention, detection, and prosecution. We are especially pleased that a large number of federal agencies are members of this task force, including the National Credit Union Administration (NCUA).

CUNA has been very proactive in providing educational materials on identity theft for our members, as well as communicating our members' concern to both the Federal Trade Commission (FTC) and the National Credit Union Administration (NCUA). These efforts include providing information on our website and through other means, which includes information that credit unions may share with their members who have experienced or are concerned about identity theft. CUNA has also recently met with the FTC to discuss means in which CUNA can promote the "Deter, Detect, and Defend" campaign that the FTC recently initiated, and we would certainly welcome additional opportunities to meet with the FTC, NCUA, as well as other government agencies in a coordinated effort to address the problem of identity theft. CUNA has also submitted a number of comment letters to the FTC and NCUA in response to the regulatory proposals that have been issued to address identity theft, as required under the FACT Act.

CUNA believes that one significant means in which to address the problem of identity theft is to focus on the underlying problem of data security vulnerabilities. These vulnerabilities have resulted in a rapidly growing number of security breaches that have occurred in recent years, which can often lead to identity theft. We urge the federal government to work more closely with card issuers, financial institutions and consumers to focus on the security breach problem. One way to accomplish this goal of bringing the principal stakeholders together would be for the federal government, under the auspices of the Task Force, to hold a "summit" and invite stakeholders to address concerns and offer recommendations to help safeguard financial data.

We recognize that Congress has been and will continue to review the issue of security breaches that compromise the confidentiality of financial information

of credit unions and their members. CUNA believes that any new legislation that addresses this issue should include the following provisions:

- Merchants or their agents, such as processors, must be prohibited from storing personal and financial information in connection with credit or debit card transactions;
- When a breach occurs involving a merchant, the company must provide useful and timely notice to financial institutions identifying the source and time of the breach, as well as the information that was compromised, which is necessary in order for financial institutions to provide the appropriate notification to those consumers who may suffer substantial harm or inconvenience as a result of the breach;
- Merchants must reimburse the consumer or financial institution on a timely basis for the cost of any notices and any losses they suffer as a result of a breach;
- Financial institutions should not be held liable if they reasonably conclude that the misuse by others of the illegally acquired information is unlikely to occur, such as when the information has been encrypted; and
- Standards regarding data security requirements for the handling of personal and financial information should be uniform and provide adequate consumer protections.

With regard to any new legislation or regulation that is intended to address identity theft, we strongly encourage Congress and the regulators to take into account the numerous regulatory requirements that have already been implemented within the last several years. These include the Gramm-Leach Bliley Act, the Bank Secrecy Act, the USA PATRIOT Act, as well as the FACT Act. To the extent that new legislation, regulation, or guidance is determined to be necessary, we strongly believe it should be risk-based, to take into account the size and complexity of those that must comply with these new requirements, and flexible in order to accommodate future changes in technology.

In addition to merchants, we believe other parties should continue to be involved in this effort to reduce identity theft. These include software companies and internet service providers, who should all play a role in protecting consumers against phishing and other forms of Internet fraud that can lead to instances of identity theft.


The Task Force has specifically requested comment as to whether there should be a review of the impact and effectiveness of the requirements imposed under the FACT Act. Because of the significant burdens imposed under the FACT Act, we strongly support such a review, as well as a review of other regulatory burdens in this area. Although a number of government agencies conduct periodic regulatory reviews, we believe special emphasis should be placed on reducing the cumulative burdens associated with the

FACT Act rules. The first such review should take place within the next year or two and future reviews should be conducted periodically thereafter.

We also support efforts that will help law enforcement to prosecute those that commit identity theft. In addition, we believe it would be helpful to publicize the law enforcement activities and accomplishments in this area. This will help assure the public, credit unions, and others that the Internet can be a safe place to conduct financial transactions, which is vital as electronic commerce has become an increasingly important component of our economy.

Thank you for the opportunity to comment on these identity theft issues. If you or your staff have questions about our comments, please give Senior Vice President and Deputy General Counsel Mary Dunn or me a call at (202) 638-5777.

Sincerely,

A handwritten signature in black ink, appearing to read "Jeffrey Bloch", is written over a light blue rectangular background.

Jeffrey Bloch
Senior Assistant General Counsel